

UNITED STATES DISTRICT COURT

for the
Central District of California

In the Matter of the Search of

(Briefly describe the property to be searched or identify the
person by name and address)

Case No. 2:24-MJ-05788

The premises located at 16178 Eastridge Court,
Chino Hills, California 91709

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California:

See Attachment A-1

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal:

See Attachment B-1

Such affidavit(s) or testimony are incorporated herein by reference.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

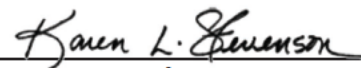
Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for ____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: September 23, 2024 @ 2:07 p.m.


Judge's signature

City and state: Los Angeles, CA

Hon. Karen L. Stevenson, United States Magistrate Judge
Printed name and title

AUSA: Jeremy K. Beecher (x5429)

Printed name and title

ATTACHMENT A-1

PREMISES TO BE SEARCHED

The premises located at 16178 Eastridge Court, Chino Hills, California 91709 ("SUBJECT PREMISES 1"). SUBJECT PREMISES 1 is located on the West side of Eastridge Court. SUBJECT PREMISES 1 is further described as a two-story residence consisting of stucco exterior walls, with iron and stucco sided fencing enclosing the property, as is pictured below. SUBJECT PREMISES 1 includes all vehicles, storage facilities, outbuildings and garages within the curtilage of the SUBJECT PREMISES 1.



ATTACHMENT B-1

(SUBJECT PREMISES 1-4 and 6; the SUBJECT VEHICLE;

SUBJECT PERSONS 1-4)

ITEMS TO BE SEIZED

1. The items to be seized are the evidence, fruits, and instrumentalities of violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute and distribution of cocaine, methamphetamine, and heroin), 21 U.S.C. § 846 (conspiracy to possess with intent to distribute and distribution of cocaine, methamphetamine, and heroin), 21 U.S.C. § 843(b) (unlawful use of a communication facility to facilitate distribution of Cocaine, methamphetamine, and heroin), 18 U.S.C. § 1956 (money laundering), and 18 U.S.C. § 924(c) (possession of a firearm in furtherance of a drug trafficking crime) (the "Subject Offenses"), namely:

- a. Cocaine, methamphetamine, and heroin;
- b. Items and paraphernalia for the manufacturing, distributing, packaging, sale, or weighing of cocaine, methamphetamine, and heroin;
- c. Firearms, ammunition, silencers, firearm parts and accessories, and items and/or material used to manufacture firearms;
- d. Items used in the packaging of currency for consolidation and transportation, such as money-counting machines, money wrappers, carbon paper, rubber bands, duct tape or wrapping tape, plastic wrap or shrink wrap, and plastic sealing machines;

e. Documents and records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with co-conspirators, sources of supply of controlled substances or firearms, or drug or firearms customers, including calendars, address books, telephone or other contact lists, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs, guns, or ammunition, were bought, sold, or otherwise distributed, whether contained in hard copy correspondence, notes, emails, text messages, photographs, videos (including items stored on digital devices), or otherwise;

f. Books, records, correspondence, ledgers, logs, journals, accounts payable and receivable, pay-owe sheets, contracts, letters and memoranda of agreements between potential co-conspirators, formulas, receipts, phone records, phone books, address books, notations and other papers, and any files relating to the transmission and exchange of cryptocurrency and/or other monetary instruments;

g. Indicia of occupancy, residency, and/or ownership of the previously described property, premises, or vehicles, including utility and telephone bills, canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, envelopes, registration, receipts, and keys which tend to show the identities of the occupants, residents, and/or owners;

h. Records concerning the use of commercial mail receiving agencies and/or post office boxes;

i. Financial records, including bank statements, bank receipts, passbooks, bank checks, money market or similar accounts, money drafts, letters of credit, payroll documents, employer information, income and expense records, Federal and State income tax returns, money orders, cashier's checks, loan applications, credit card records, safe deposit box and records, acquisitions, notes, and records reflecting vehicles, aircraft or vessels owned, purchased, sold or leased;

j. United States currency, and records relating to income derived from money laundering and expenditures of money and wealth, for example, money orders, wire transfers, cashier's checks and receipts, passbooks, cash cards, gift cards, checkbooks, check registers, securities, precious metals, jewelry, antique or modern automobiles, bank statements and other financial instruments, including stocks or bonds in amounts indicative of money laundering;

k. Storage units and containers, such as floor safes, wall safes, upright safes (also known as gun safes), lock boxes, and other self-contained locked enclosures;

l. Documents indicating travel in interstate and foreign commerce to meet with clients and/or co-conspirators, such as travel itineraries, plane tickets, boarding passes, motel and hotel receipts, passports and visas, credit card receipts, and telephone bills;

m. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

2. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. applications, programs, software, documentation, manuals, passwords, keys, and other access devices that may be necessary to access the device or data stored on the device, to run software contained on the device, or to conduct a forensic examination of the device;

g. records of or information about Internet Protocol addresses used by the device.

3. As used herein, the terms "records," "information," "documents," "programs," "applications," and "materials" include records, information, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

4. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

5. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

6. As used herein, the term "digital devices" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communications devices, such as telephone paging devices, beepers, cellular telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

SEARCH PROCEDURE FOR DIGITAL DEVICES

7. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The

government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the scope of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase," "Griffeye," and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the scope of items to

be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the scope of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the scope of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

8. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel

assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

9. During the execution of this search warrant, law enforcement is permitted to: (1) depress the holder's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the holder's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

10. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.